

(U) Glossary

Terms That Have Bearing Upon the FBI's National Foreign Intelligence Program



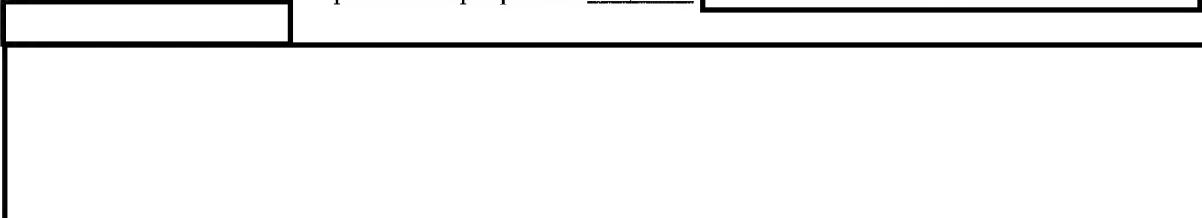
3. (U) Agent: (a) A person who engages in clandestine intelligence or TI activities under the direction of an intelligence or terrorist organization, but who is not an officer, employee or cooptee of that organization. (b) An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence, CI or CT purposes. (c) A person who is authorized or instructed to obtain, or assist in obtaining, information for intelligence or CI purposes.



6. (U) Analysis: The process in which intelligence information is subjected to systematic examination in order to identify significant facts, and derive conclusions therefrom.

7. (U) Assessment: (a) An appraisal of the worth of an intelligence activity, source, information or product, in terms of its contribution to a specific goal. (b) An appraisal of the credibility, reliability, pertinency, accuracy or usefulness of information in terms of an intelligence need. (c) A judgment of motives, qualifications and characteristics of present or prospective employees, Agents or Assets.

8. (U) Asset: Any resource (human, technical or otherwise) available to an intelligence, CI, IT or security service, for operational purposes. See, also:



10. (U) Asylum: An immigration status which is sought by one who seeks to remain in the U.S. because of persecution or anticipated persecution in his/her country of origin.

11. (U) (REL TO) Authorized For Release To: A control marking which is used when a limited exception to the parameters of NOFORN may be made, to allow the release of information

~~SECRET NOFORN~~

beyond U.S. recipients. *See: Director of Central Intelligence Directive 1/7, Section 9.5.*

15. (U) Briefing: The preparation of an individual for a specific operation, by describing the objectives, the methods to be employed, and the situation(s) which will be encountered.

17. (U) Buckley Amendment: Governs the acquisition of education records from educational agencies and institutions. *See: Title 20, U.S. Code, Section 1232g.*

19. (U) PROPIN (Caution--Proprietary Information Involved): A marking used, with or without a security classification, to identify information which has been provided under an express or implied understanding that the information will be protected as a proprietary trade secret, or proprietary data, believed to have actual or potential value. *See: Director of Central Intelligence Directive 1/7, Section 9.3.*

20. (U) Caveated Information: Information that is subject to an authorized control marking. *See: id., Section 3.1.*

(S)

24. (U) Chief Of Mission: The principal officer in charge of a diplomatic mission of the U.S., or of a U.S. office abroad which is designated by the Secretary of State as diplomatic in nature. See: Title 22, U.S. Code, Section 3902(3).

(S)

27. (U) Cipher: Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text, and/or in which units of plain text are rearranged. See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary.

29. (U) Clandestine Operation: A preplanned intelligence collection activity, or covert political, economic, propaganda, or paramilitary action, which is conducted in such a way as to assure the secrecy of the operation.

(C)

31. (U) Classification: The determination that official information requires, in the interest of National Security, a specific degree of protection against disclosure, coupled with a designation signifying that such a determination has been made.

32. (U) Codename: A single word which is used to disguise the identity of a covert operative. Code names are reserved for:

33. (U) Codeword: (a) Any two words which are used to disguise certain covert operations; e.g. [REDACTED] all undercover operations. (b) Any single word or term which is used with a security classification to indicate that material so classified was derived through a sensitive source or method, constitutes a particular type of SCI, identifies a particular investigation, and/or is otherwise accorded limited distribution.

b7E

34. (U) Coercion: An expressed or implied threat, made to elicit a desired response or action from a person.

35. (U) Collection Requirement: A request for a specific collection action, in order to satisfy a general or specific intelligence information need.

(C)

[Redacted]
38. (U) COMINT (Communications Intelligence): An intelligence product, derived from [Redacted]

39. (U) COMSEC (Communications Security): Measures and controls taken to deny unauthorized persons information derived from telecommunications, and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security and physical security of COMSEC material. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary; and Manual of Investigative Operations and Guidelines, Section II, 16-12.*

(S)

[Redacted]
42. (U) Compartmentation: The restriction of information to those who have a need-to-know.

43. (U) Compromise: A disclosure of information to unauthorized persons; or a violation of the security policy of a system in which unauthorized, intentional or unintentional disclosure, modification, destruction or loss of an object may have occurred. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary.*

44. (U) Concealment Device: An innocuous object, designed or adapted as a container for secreting materials and/or equipment.

45. (U) Contact: A person who has met with the subject of an FCI, IT or foreign intelligence investigation.

[Redacted]
48. (U) Controlled Technology: Referring to all forms of restricted and embargoed unclassified technology.

51. (U) Counterespionage: An aspect of FCI, designed to detect, destroy, neutralize, exploit and/or prevent espionage activities through identification, penetration, manipulation, deception and/or repression of individuals, groups or organizations which are conducting or suspected of conducting espionage activities.

52. (U) Counterintelligence Policy Board: Serves as the principle mechanism for (a) developing policies and procedures for the approval of the President to govern the conduct of CI activities; and (b) resolving conflicts, as directed by the President, which may arise between elements of the U.S. Government which carry out such activities.

53. (U) Countermeasure: An action taken to negate the opposition's ability to take advantage of its target's vulnerabilities.

54. (U) Counterterrorism: Measures taken to prevent, deter and respond to a terrorist act, or the threat of such an act, but not including personnel, physical, document or communications security programs. *See: Executive Order 12333, Section 3.4(a).*

56. (U) Covert Action: An operation which is designed to influence governments, events, organizations or persons, and which is planned and executed in such a manner as to conceal the identity of the sponsoring power, or to permit plausible denial.

58. (U) Critical Technology: Any technology, selected on the basis of its ability to (a) enhance U.S. national and economic prosperity, (b) provide for U.S. economic independence and competitiveness in the global marketplace, (c) contribute to a rising standard of living, (d) strengthen the U.S.' industrial base, and/or (e) provide for an increased National Security capability. *See: the March 1991, and the January 1993 reports of the National Critical Technologies Panel.*

59. (U) Cryptanalysis: The conversion of an encrypted message to plain text, without the knowledge of the crypto-algorithm and/or key which was employed in the encryption. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary.*

60. (U) Cryptographic Systems. *See: Manual of Investigative Operations and Guidelines, Section II, 16-12.1.*

[Redacted]

[Redacted]

65. (U) Dead Drop: An unattended place to which communications, materials or equipment can be taken by one individual, and from which they can be retrieved by another individual, without the two either meeting or seeing each other.

66. (U) Debriefing: A nonhostile interview of an individual who has completed an intelligence assignment, or who has knowledge (through observation, participation or otherwise) of operational or intelligence significance.

67. (U) Deception (Disinformation): A measure designed to induce an opponent into taking an action which is prejudicial to its own interests.

68. (U) Deep Cover Operation: Any undercover operation which

[Redacted]

69. (U) Defector: A person of any nationality (though usually a country whose interests are hostile or inimical to those of the U.S.) who has escaped from the control of his/her home country; who is unwilling to return to that country; and who is of special value to the U.S. government because (a) he/she is able to add valuable new or confirmatory information to U.S. intelligence knowledge; (b) he/she is or has been of operational value to a U.S. department or agency; or (c) the defection can be psychologically exploited to the advantage of the U.S. *See: Director of Central Intelligence Directive 4/1, Section 2.a.*

70. (U) Defector Source: An individual who (a) possesses intelligence information of value, who (b) has either openly, or without announcement, left the employment of his/her own country's government, and who (c) is furnishing information to another country's government.

71. (U) Delegation: A group [Redacted] which has been admitted to the U.S. as a representative of an organization or corporation [Redacted]

72. (U) Designated Personnel: Within the Arms Control Treaty arena, officials who participate in (a) Coordinating Group meetings, which are held at each U.S. nuclear test; or (b) on-site activities at the Nevada Test Site and the Designated Seismic Sites.

73. (U) Diplomatic Establishment: Any establishment which is directed and controlled by a foreign government, and which deals with diplomatic, commercial, cultural, educational, news-gathering and/or tourism affairs.

74. (U) Diplomatic Officials: Personnel employed by a country, who act in official capacities. E.g., (a) diplomats, attaches and consuls assigned to diplomatic missions, embassies and Consulates General; and (b) members of international organizations or establishments who are assigned to the U.S. for a period of one year or more. Immediate family members, servants and personal employees are excluded from this class unless unusual circumstances exist. [Redacted]

[Redacted]

75. (U) Diplomatic Pouch (Diplomatic Bag): A container, bearing visible marks of its

~~SECRET~~

diplomatic character, and protected from opening or detention by a treaty to which the U.S. is a party. See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.B.

76. (U) Dissemination: The timely distribution of an intelligence product, in a form suitable to intelligence consumers.

77. (U) ORCON (Dissemination and Extraction of Information Controlled by Originator): A security designation which is used to enable the originator of intelligence to control its wider distribution and use on a continuing basis. See: Director of Central Intelligence Directive 1/7, Section 9.2.

79. (U) Double Agent: An Asset who is actively cooperating with, receiving assignments from, and/or performing tasks for a foreign power as a clandestine agent; or who seeks to achieve such a relationship; but who is actually under the control of another, opposing service.

b7E

82. (U) Dual Use Technology: Technology that has both civilian and military applications.

83. (U) Economic Espionage: Foreign power-sponsored or coordinated intelligence activity directed at the U.S. Government, U.S. corporations, establishments or persons, which involves (a) the unlawful or clandestine targeting or acquisition of sensitive financial, trade or economic policy information, proprietary economic information, or critical technologies; or (b) the unlawful or clandestine targeting or influencing of sensitive economic policy decisions.

(S)

85. (U) Electronic Surveillance: (a) The acquisition (by electronic, mechanical or other surveillance device) of the contents of any wire or radio communication (sent by, or intended to be received by, a U.S. person in the U.S.), if the contents are acquired by intentionally targeting that U.S. person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (b) the acquisition (by electronic, mechanical or other surveillance device) of the contents of any wire or radio communication (to or from a person in the U.S.), without the consent of any party thereto, if such acquisition occurs in the U.S.; (c) the intentional acquisition (by an electronic, mechanical, or other surveillance device) of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the U.S.; or (d) the installation or use of an electronic, mechanical, or other surveillance device in the U.S. for monitoring to acquire information (other than from a wire or radio communication), under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. See: Title 50, U.S. Code, Section 1801(f).

b1
Referral/Consult~~SECRET//QFORN~~

~~SECRET~~

86. (U) Embargoed Material: Material which is formally prohibited by U.S. law and administrative procedure from being transferred to certain recipients.

87. (U) Emigre: A person who departs from his/her country for any lawful reason, with the intention of permanently resettling elsewhere. *See: Director of Central Intelligence Directive 4/1, Section 2(g).*

88. (U) Espionage: Intelligence activity directed toward the acquisition of intelligence through clandestine means. *See: Director of Central Intelligence Directive 5/1, Section 2.*

b7E

90. (U) Fair Credit Reporting Act: Governs the acquisition of consumer reports from consumer reporting agencies. *See: Title 15, U.S. Code, Sections 1681-1681f.*

b7E

93. (U) For Or On Behalf Of A Foreign Power: Referring to a determination of the extent to which a foreign power is involved in the (a) control, leadership or policy direction; (b) financial or material support; or (c) leadership, assignments or discipline of an individual or group. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.L.*

94. (U) FCI (Foreign Counterintelligence): Information gathered, and activities conducted, to protect against espionage and other intelligence activities, sabotage, or assassinations conducted by, for or on behalf of foreign powers, organizations or persons, or IT activities--but not including personnel, physical, document or communications security programs. *See: Executive Order 12333, Section 3.4(a) and AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.D.*

(S) -----

96. (U) Foreign Diplomatic Establishment: An embassy, mission, consulate, residential compound or other premises owned or leased and used for official purposes by a foreign government, whether or not recognized by the U.S.; premises of international organizations, as defined by Title 22, USC, Section 288; premises of establishments authorized to be treated as international organizations or diplomatic missions by specific statute (e.g., Title 22, USC, Section 288f-1 through 288i); and the premises of establishments of foreign representatives to such international organizations. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.E.*

97. (U) Foreign Intelligence: Information relating to the capabilities, intentions and activities

~~SECRET//NOFORN~~

b1
Referral/Consult

~~SECRET~~

of foreign powers, organizations or persons--but not including counterintelligence except for information on IT activities. *See: Executive Order 12333, Section 3.4(d).*

98. (U) **Foreign Intelligence Agent**: A person (other than a foreign IO) who is engaged in intelligence activities or sabotage for or on behalf of a foreign power, or IT activities, or who knowingly conspires with or aids or abets such a person in such activities. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.G.*

99. (U) **Foreign Intelligence Officer**: A member of a foreign intelligence service. *See: id. Section II.H.*

100. (U) **(FISA) Foreign Intelligence Surveillance Act**: Governs electronic surveillances and physical searches in FCI, international terrorism and foreign intelligence investigations. *See: Title 50, U.S. Code, Sections 1801-1829, 1841-1846 and 1861-1863.*

101. (U) **Foreign Intelligence Surveillance Court**: A body of seven federal district court judges who have jurisdiction to hear applications, and to grant orders for, electronic surveillances and physical searches under the FISA.

102. (U) **Foreign Language Committee**: Serves as the focal point with the IC, and between the IC and other elements of the U.S. Government, academia and the private sector for the coordination of IC foreign language efforts. *See: Director of Central Intelligence Directive 3/15.*

103. (U) **Foreign Liaison Officer**: A government official who has been accredited to represent that government in the exchange and/or discussion of intelligence.

b7E

105. (U) **Foreign Official**: A foreign national in the U.S. who is (a) acting in an official capacity for a foreign power, (b) attached to a foreign diplomatic establishment or an establishment under the control of a foreign power, or (c) employed by an international organization established under an agreement to which the U.S. is a party.

106. (U) **Foreign Power**: (a) A foreign government or any component thereof, whether or not recognized by the U.S. (b) A faction of a foreign nation or nations, not substantially composed of USPERs. (c) An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. (d) A group engaged in IT or activities in preparation therefor. (e) A foreign-based political organization, not substantially composed of USPERs. (f) An entity that is directed and controlled by a foreign government or governments. *See: Title 50, U.S. Code, Section 1801.*

107. (U) **Foreign Visitor**: A foreign national in the U.S. who is not a PRA of the U.S. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.K.*

108. (U) **FOUO**: A marking, used on classified intelligence, which alerts readers that the information either clearly identifies, or would reasonably permit ready identification of, intelligence sources or methods that are particularly susceptible to countermeasures that would either nullify or measurably reduce their effectiveness. *See: Director of Central Intelligence Directive 1/7 Supplement.*

109. (U) **Front**: An organization or company which is used by an FIS or IT group as a guise, to protect clandestine intelligence or terrorist activities.

~~SECRET//NOFORN~~

~~SECRET~~

(S)



b1

111. (U) HUMINT (Human Intelligence): Intelligence information that is collected from human sources, in either an overt or clandestine manner. *See: Director of Central Intelligence Directive 3/7, Section 2.*



b7E

113. (U) Illegal Transfer: The transfer of controlled, but unclassified technology.

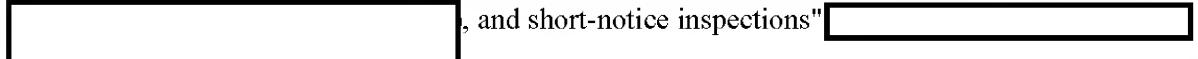


b1

115. (U) Information Handling Committee: In consultation with the Executive Director for Intelligence Community Affairs, advises the DCI on the establishment of common objectives for USIC information handling, and coordinates the achievement of these objectives through improvement and integration of USIC information handling systems. *See: Director of Central Intelligence Directive 3/14.*



117. (U) Inspectors: Within the Arms Control Treaty arena, officials who, at U.S. locations described in the Intermediate-Range Nuclear Forces Treaty Protocol, participate in "eliminations"



b7E

~~SECRET//NOFORN~~

119. (U) Intelligence: (a) Referring, collectively, to the functions, activities or organizations that are involved in the process of planning, gathering and analyzing information of potential value to decision makers. (b) The product which results from the collection, collation, evaluation, analysis, integration and interpretation of collected information.

120. (U) Intelligence Activity: An activity conducted by, for or on behalf of a foreign power, for intelligence purposes, or to affect political or governmental processes. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.M.*

121. (U) Intelligence Community: All components of a government which cooperate in the production of intelligence and CI. Within the U.S., it includes: (a) the CIA; (b) the NSA; (c) the DIA; (d) reconnaissance program offices within the DOD; (e) DOS's Bureau of Intelligence and Research; intelligence elements of (f) the Army, (g) the Navy, (h) the Air Force, (i) the Marine Corps, (j) the FBI, (k) the Department of the Treasury and (l) the DOE; and (m) staff elements of the DCI. *See: Executive Order 12333, Section 3.4(f).*

122. (U) Intelligence Community Executive Committee: The DCI's principal IC advisory body concerning: (a) intelligence policy and planning; (b) resource management; (c) intelligence requirements, management and evaluation and (d) such other matters as may be referred to it by the DCI. *See: Director of Central Intelligence Directive 3/2.*

123. (U) Intelligence Officer: A professionally trained member of an intelligence service.

124. (U) Intelligence Oversight Board: An organization which: (a) reports to the President and the AG on USIC activities which may be unlawful, or contrary to EO or Presidential Directive; (b) reviews the internal guidelines of agencies within the USIC which concern intelligence activities and the law; (c) reviews the practices and procedures of agencies within the USIC for discovering and reporting intelligence activities that may be unlawful or contrary to EO or Presidential Directive; and (d) conducts such investigations as it deems necessary to carry out the aforementioned functions. *See: Executive Order 12863*

(S)

126. (U) International Terrorism: Activities that (a) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any State, or that would be a criminal violation if committed within the jurisdiction of the U.S. or any State; (b) appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by assassination or kidnapping; and (c) occur totally outside the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.N.*

127. (U) International Terrorist: An individual or group that knowingly engages in IT or activities in preparation therefore, or knowingly aids or abets any person engaged in such activities. *See: id. Section II.O.*

128. (U) Inviolable Premises: Diplomatic or consular premises, including the residences of diplomatic agents, administrative and technical personnel, consular officers or consular employees,

b1
Referral/Consult

~~SECRET//NOFORN~~

~~SECRET~~

and any international organization premises, including residences [redacted]

(S)

133. (U) Logical Sources of Information: Individuals who, by virtue of status or occupations, are believed to be in positions to provide valuable information regarding the subjects of FIs.

(S)

138. (U) National Counterintelligence Operations Board: An entity composed of personnel on the National Counterintelligence Policy Board, which operates closely with NACIC in resolving specific issues which are brought before it by the NACIPB.

139. (U) National Counterintelligence Policy Board: A senior CI policy coordination body, composed of senior executives from: the FBI; DOD; the CIA; DOS; DOJ; the NSC; and OMB.

140. (U) National Foreign Intelligence Board: The DCI's senior IC body, providing him/her advice on: (a) production, review and coordination of national foreign intelligence; (b) interagency

~~SECRET//NOFORN~~

b1
b7E

exchanges of foreign intelligence information; (c) arrangements with foreign governments on intelligence matters; (d) protection of intelligence sources and methods; (e) activities of common concern; and (f) such other matters as may be referred to it by the DCI. *See: Director of Central Intelligence Directive 3/1.*

141. (U) National Foreign Intelligence Program: Includes (a) the programs of the CIA; (b) the programs of the Consolidated Cryptologic Program; (c) the General Defense Intelligence Program, (d) the programs of offices within the DOD for the collection of specialized national foreign intelligence through reconnaissance (except such elements as the DCI and the Secretary of Defense agree should be excluded); (e) the foreign intelligence and FCI programs of other agencies within the USIC; (f) activities of the staff elements of the DCI. Activities to acquire the intelligence required for the planning and conduct of tactical operations by the U.S. military forces are not included in the NFIP. *See: Executive Order 12333, Section 3.4(g).*

(C)

(S)

145. (U) National Security Letter: A process used to obtain telephone toll records, subscriber information, financial records, and consumer credit reports on subjects of FCI, foreign intelligence, and IT investigations, where the appropriate statutory predicates have been met.

146. (U) National Security Telecommunications and Information Systems Security Committee: An organization which operates under the direction of the U.S. Government's System Security Steering Committee; which consists of the Secretaries of Defense, State, and the Treasury, the AG, the Director of the Office of Management and Budget, and the DCI. Consisting of representatives from the Departments of Defense, State, Treasury, Commerce, Transportation, and Energy; the Joint Chiefs of Staff, GSA, FBI, Army, Navy, Air Force, Marine Corps, DIA, CIA and NSA. The NSTIISCC develops operations policies, and provides guidance to government agencies as respects computer security.

147. (U) Need-to-Know: A determination by an authorized holder of classified information that access to that material is required by another person to perform a specific and authorized function. The recipient must possess an appropriate security clearance, and approvals in accordance with DCID 1/14. *See: Director of Central Intelligence Directive 1/19, Section 1.1.12.*

[Redacted]

150. (U) Non-U.S. Person: An undocumented alien, or a foreign national lawfully in the U.S. who is not a PRA. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.P.*

151. (U) NOFORN (Not Releasable To Foreign Nationals): A security designation which is used to identify classified intelligence which may not be released, in any form, to foreign governments, foreign nationals or non-U.S. citizens, without the originator's permission. *See: Director of Central Intelligence Directive 1/7, Section 9.4.*

[Redacted]

154. (U) Official Establishment: Any establishment controlled by a foreign government, regardless of its diplomatic or non-diplomatic status.

155. (U) Open Storage: The storage of classified information within an accredited facility (though not within GSA-approved containers) while the facility is unoccupied by authorized personnel. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary.*

[Redacted]

157. (U) OPSEC (Operations Security): The process of detecting activities which, by themselves or combined with other data, may reveal the existence of sensitive information or operations.

158. (U) Otherwise Illegal Activity: Any activity which would be illegal but for the fact of its having been appropriately authorized. *See: AG Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, CI or IT Intelligence Investigations.*

[Redacted]

163. (U) Permanent Resident Alien: A person who has received lawful permanent resident status in the U.S., but who is not yet a U.S. citizen.

164. (U) Persona Non Grata: An official act, declaring a foreign national unacceptable or

unwelcome--usually when found to have been engaging in intelligence activities, or otherwise violating the law.

165. (U) Physical Search: Any physical intrusion within the U.S. into premises or property (including an examination by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes. *See: Title 50, U.S. Code, Section 1821(5).*

166. (U) PL 110 (Public Law 110): A law whereby vetted Defectors are granted PRA status through agreement between the DCI, the Commissioner of INS and the AG.

(S)

b1

168. (U) President's Foreign Intelligence Advisory Board: An entity which (a) assesses the quality, quantity and adequacy of U.S. intelligence and CI activities; (b) reports to the President regarding the USIC's objectives, conduct, management and efforts at coordination; and (c) makes such recommendations as may be appropriate. *See: Executive Order 12863, Sections 1.2 through 104.*

169. (U) Proprietary Economic Information: Any economic, scientific or technical information, design, process, procedure, formula, strategy or improvement (whether represented in a tangible or intangible form) which is not generally accessible or known in the trade, business or scientific communities, and concerning which the owners have taken affirmative measures to prevent its entry into the public domain.

170. (U) Proprietary Enterprise: A sole proprietorship, partnership, corporation or other business entity which is created, owned or controlled, directly or indirectly by the FBI, in order to support an undercover operation, and whose relationship with the FBI is concealed.

b7E

171. (U) Proprietary Information and Technology: Sensitive material that is not yet embargoed or classified.

172. (U) Publicly Available: Information which (a) has been published or broadcast for general public consumption, (b) is available on request to any member of the general public, (c)

could lawfully be seen or heard by any casual observer, or (d) is made available at a meeting open to the general public. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.R.*

b7E

174. (U) Recommendations: Assets who have been recommended to the FBI by (i) another Asset, (ii) another U.S. Government agency, or (ii) a foreign intelligence service.

175. (U) Recruitment: The process of enlisting a person to work for an intelligence or CI service.

b7E

178. (U) Refugee: A person who (a) has departed his/her country of nationality or habitual residence; who (b) is unable to return to that country because of a well-founded fear of being persecuted for reasons of race, religion, nationality, membership in a particular social group, or political opinion; who (c) does not possess another citizenship; and who (d) has not acquired resident status in the country of present domicile. *See: Director of Central Intelligence Directive 4/1, Section 2.c.*

b7E

180. (U) Residency--Illegal: An intelligence establishment, which has no overt connection with government.

181. (U) Residency--Legal: An intelligence establishment, which is overtly linked to its government.

182. (U) Right to Financial Privacy Act: Governs the acquisition of financial records of customers of financial institutions. *See: Title 12, U.S. Code, Sections 3401-3414.*

183. (U)

b7E

(S)

(S)

186. (U) **Secondary Contacts**: Assets who, though not the subjects of investigations, were interviewed and thus found to be amenable to cooperating with the FBI.

187. (U) **SCI (Sensitive Compartmented Information)**: Classified information (concerning or derived from intelligence sources, methods, or analytical processes) which is required to be handled within formal access control systems established by the DCI. *See: Director of Central Intelligence Directive 1/19, Section 1.1.18.*

188. (U) **SCIF (Sensitive Compartmented Information Facility)**: An accredited area, room, group of rooms, building or installation where SCI may be stored, used, discussed and/or processed. *See: Director of Central Intelligence Directive 1/19, Section 1.1.15.*

189. (U) **Sensitive Financial, Trade And Economic Policy Information**: Data, details, facts and/or knowledge, concerning strategy, methods, tactics and/or procedures; which pertain to productivity, strategic goals, financial planning and allocation of resources, of the U.S. government, U.S. corporations, establishments and/or persons; which is not generally accessible or known in the financial, trade, business or scientific community, the owners of which have taken affirmative measures to prevent its entry into the public domain.

190. (U) **SIGINT (Signals Intelligence)**: An intelligence product, derived from the monitoring of radio transmissions of all kinds; e.g., teletype; Morse code; radiophone; radar emissions; and signals from missiles, satellites and spacecraft.

191. (U) **Sleeper**: An Illegal or Agent, residing in a foreign country, and under orders to engage in no intelligence activities until a specific need arises.

192. (U) **SAP (Special Access Program)**: Any program, established under EO 12356, which imposes controls governing access to classified information above and beyond those required by normal management and safeguarding practices.

b7E

194. (U) **Substantially Composed Of U.S. Persons**: In determining whether a group or organization is substantially composed of USPERS

b7E

See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.T.

(S)

(S)

198. (U) Terrorist: An individual who engages in terrorist activities which are intended to (a) intimidate or coerce a civilian population; (b) influence the policy of a government by intimidation or coercion; or (c) affect the conduct of a government by assassination or kidnapping.

199. (U) Threat Analysis: A comprehensive assessment of the threat posed not only by an opposition intelligence service, but also those organizations and individuals whose interests are inimical to those of the U.S.

b7E

201. (U) Training Directors' Consortium: Serves as the focal point within the IC, and between the IC and other U.S. Government elements, on training and educational requirements, programs, policies and resources of common concern. *See: Director of Central Intelligence Directive 3/27.*

202. (U) Transport Personnel: Within the Arms Control Treaty arena, officials who transport or accompany Designated Personnel and/or equipment to and from Russia and the U.S. Transport Personnel do not participate in verification activities, and are not permitted to travel beyond designated points of entry.

b7E

205. (U) Undercover Operation: Any situation in which a Special Agent or Support Employee is engaged in a relationship with the target of a FCI, IT or foreign intelligence investigation, where the contact is expected to continue over a period of time, and where FBI employment is concealed. A "Group I" operation involves sensitive circumstances; whereas a "Group II" operation is non-sensitive.

206. (U) Undercover Special Agent/Support Person: An FBI employee who is acting in an undercover capacity.

207. (U) UDP (Undisclosed Participation): Joining or otherwise participating in any organization in the U.S., on behalf of an agency within the US IC, without disclosing the IC tie to an appropriate official of that organization. *See: Executive Order 12333, Section 2.9; and AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section IV.A.*

208. (U) United States: All areas under the territorial sovereignty of the U.S. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.V.*

209. (U) U.S. Arms Control and Disarmament Agency: Within the Arms Control Treaty

arena, is responsible for: (i) formulating, coordinating and carrying out arms control policies; (ii) conducting and coordinating research; (iii) preparing and managing U.S. participation in negotiations; and (iv) disseminating information regarding arms control matters to the general public.

210. (U) U.S. Economic Interests: Those financial, trade, research and development, technological and policy issues which define U.S. strategic economic goals, including: (a) the maintenance of U.S. economic health, (b) providing a higher standard of living, and (c) organizing a sustainable economic order.

(S)

214. (U) USPER (U.S. Person): A U.S. citizen; a PRA; an unincorporated association, substantially composed of U.S. citizens or permanent resident aliens; or a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. *See: Executive Order 12333, Section 3.4(i); and AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.W.*

215. (U) Volunteers: (a) Assets who approach the FBI offering to provide information.

b7E

~~SECRET~~

(S)

EFFECTIVE DATE: 04/19/2002 MCRT# 1262 Div: D5 CAV: NF SECCLASS: ~~SECRET~~

b1
b7E
Referral/Consult

~~SECRET//NOFORN~~